Opinnäytetyö (AMK)

Tietotekniikan koulutusohjelma

Ohjelmistotuotanto

2011

Jani Rikström

WLAN-SALAUSAVAINTEN PURKU

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietotekniikan koulutusohjelma | Ohjelmistotuotanto

Joulukuu 2011 | 32

Ohjaaja Tiina Ferm

Jani Rikström

WLAN-SALAUSAVAINTEN PURKU

Tässä opinnäytetyössä selvitetään langattomien lähiverkkoon tarjottavien suojausmenetelmien turvallisuutta ja langattoman lähiverkon tietoturvaa. Lisäksi selvitetään myös, miten eri käyttöjärjestelmät vaikuttavat salaukseen.

Tutkimusympäristö rakennettiin 802.11g-standardin ympärille, koska tutkimuksessa käytetyt langattomat laitteet tukevat kyseistä standardia. Tutkimuksissa käytettiin ensisijaisesti Linux-käyttöjärjestelmää, johon asennettiin aircrack-ng-ohjelma salausavaimien selvittämiseen. Siinä käytetään myös kahta minikannettavaa, joissa on käyttöjärjestelminä Windows XP ja 7.

Hyökkäysmenetelminä käytettiin välistäveto- ja sanakirja-hyökkäystä. Niitä tutkittiin hyökkäämällä WEP-, WPA- ja WPA2-salausprotokollia vastaan ensisijaisesti kuuntelemalla langattoman verkon liikennettä ja sieppaamalla nelivaiheinen kättely käyttäjän ja tukiaseman väliltä.

Lopputuloksena selvisi, että WEP-salausprotokolla on helposti murrettavissa. Molemmat WPA- ja WPA2-salausprotokollat ovat riittäviä, kun käytetään tarpeeksi pitkää ja erikoista salasanaa, mutta turvallisin on WPA2-salausprotokolla, joka käyttää AES-salausta. Tulosten perusteella kotikäyttäjät voivat hyödyntää tietoa ja suojata näin ollen langattoman lähiverkkonsa paremmin tietoturvahyökkäyksiltä.

ASIASANAT:

WLAN, Linux, WEP, WPA, WPA2, Aircrack-ng

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Software Engineering

December 2011 | 32

Instructor Tiina Ferm

Jani Rikström

BREAKING WIRELESS LAN ENCRYPTION KEYS

This thesis discusses the security of protection methods and wireless LAN security offered to wireless LAN. It also explains the influence of different operating systems to encryption.

The environment was built around the 802.11g standard, because the wireless devices used in the study support this standard. Linux operating system was primarily used, into which aircrack-ng program was installed or cryptographic settlement. Also two mini-laptops, with operating system Windows XP and 7 were used

As attack methods Man in the Middle and the dictionary brute force attack were used. They were looked into by attacking WEP, WPA and WPA2 encryption protocols primarily by listening to the wireless network traffic and intercepting of a four-way handshake between the user and the base station.

The results show that the WEP encryption protocol can be broken easily. Both WPA and WPA2 encryption protocols are adequate, when using a long enough and special password, but the safest is WPA2 encryption protocol, which uses the AES encryption. The results indicate that home users can take advantage of information and thus to protect the wireless local area network to improve security against attacks.

KEYWORDS:

WLAN, Linux, WEP, WPA, WPA2, Aircrack-ng

SISÄLTÖ

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET

AAA	Käyttäjän todentaminen, valtuutus ja tilastointi (Authentication, Authorization and Accounting)
AES	Kehittyneempi salausstandardi (Advanced Encryption Standard)
ARP	Protokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite (Address Resolution Protocol)
DHCP	Antaa IP-osoitteita uusille lähiverkkoon kytkeytyville laitteille (Dynamic Host Configuration Protocol)
EAP	Käyttäjän tunnistusprotokolla (Extensible Authentication Protocol)
GHz	Käytettävä radiotaajuus (Gigahertz)
HTTP	Internet-selaimien käyttämä tiedonsiirtomenetelmä (Hypertext Transfer Protocol)
IEEE	Kansainvälinen tekniikan alan järjestö (Institute of Electrical and Electronics Engineers)
MAC	Verkkosovittimen yksilöivä osoite (Media Access Control)
Mbit/s	Megabittiä sekunnissa (Megabits per second)
MIMO	Signaalin vastaanottamiseen ja lähettämiseen käytetään useampaa antennia (Multiple Input Multiple Output)
ODFM	Tiedonsiirto monilla toisiaan häiritsemättömillä taajuuskanavilla samaan aikaan (Orthogonal Frequency Division Multiplexing)
RADIUS	Käyttäjän yhdistyessä tapahtuva todentaminen (Remote Authentication Dial In User Service)
TKIP	Tietoliikenneyhteyden salaaminen ja turvaaminen (Temporal Key Integrity Protocol)
WEP	Suojaa langattoman verkon tietoliikennettä (Wired Equivalent Privacy)
WLAN	Langaton lähiverkko (Wireless Local Area Network)
WPA	Langattoman verkon tietoturvaprotokolla (Wi-Fi Protected Access)
WPA2	Langattoman verkon uudempi tietoturvaprotokolla (Wi-Fi Protected Access 2)

1 JOHDANTO

Langattomat lähiverkot ovat nykyisin todella suuressa asemassa yrityksissä, kotona ja kouluissa. Vapaasti tietokoneen kanssa liikkuminen työpaikalla tai kotona paikasta toiseen helpottaa asioiden hoitamista. Kustannukset ovat myös pienemmät kuin normaalissa langallisessa verkossa. Langattoman tekniikan käyttöönotto tuo kuitenkin myös mukanaan uusia tietoturvariskejä. Uudistunut langattoman verkon tekniikka mahdollistaa nykyään myös television liitettävyyden tietoverkkoon. Näin ollen on mahdollista käyttää Internet-palveluita televisiossa tai kuunnella tietokoneella olevaa musiikkia verkon avulla televisiossa.

WLAN (Wireless Local Area Network) -verkot tuovat paljon uusia mahdollisuuksia, mitä normaalit kiinteät verkot eivät pysty tarjoamaan. Käyttö on yleistynyt ja lisääntynyt. Tärkein osa langattomista lähiverkoista on tietoturva, koska signaalit käyttävät avointa siirtymätietä edetessään. Kun WLAN tuli markkinoille, se puhutti tietoturvallisuuden puolesta, mutta nyt asia on toinen. Se tarjoaa tehokkaita suojausmenetelmiä, mitkä riittävät liikenteen turvaamiseen verkossa. Langaton lähiverkko kannattaa suojata, jos haluaa välttyä hakkereilta tai muilta hyökkäyksiltä. Useat käyttäjät eivät välitä tai tiedä asiasta, jonka vuoksi ei suojata WLAN-verkkoja kunnolla tai ylipäänsä ollenkaan.

WLAN-verkot ovat tulleet tutuiksi opiskelun ja harrastelun yhteydessä, mitä tulee käytettyä päivittäin esimerkiksi tietokoneella tai älypuhelimella. Internetissä luki kolme vuotta sitten, että osa salausmenetelmistä on helposti murrettavissa ja siitä työ sai alkunsa. Kuinka helposti ne todella ovat murrettavissa nykypäivän tekniikalla ja ohjelmistoilla?

Tässä työssä tutkitaan, kuinka paljon langattoman verkon suojausprotokollat suojaavat. Työssä luodaan langaton lähiverkko kotiympäristöön, jossa tutkitaan, kuinka WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) ja WPA2 (Wi-Fi Protected Access 2) -salausprotokollat suojaavat kahta eri hyökkäystä vastaan. Salausavaimien murtamiseen käytetään aircrack-ng-ohjelmaa, joka on asennettu Linuxin Ubuntu-käyttöjärjestelmän omaavaan tietokoneeseen.

2 LANGATTOMAN LÄHIVERKON HYÖDYT JA HAITAT

WLAN-verkko tarkoittaa rajatun alueen, kuten ravintolan, työpaikan, kodin tai kahvilan lähiverkkoa, johon yhdistetään langattoman verkon kantoalueella olevat laitteet langattomasti.

Langaton lähiverkko on yleensä kiinteän lähiverkon korvaaja kokonaisuudessaan tai lisäys verkkoon. Jos työpaikalla on käytössä sekä kiinteä että langaton lähiverkko, voi työntekijä jatkaa töitään toisessa huoneessa langattomassa lähiverkossa ilman, että on sidottu kiinteään lähiverkkoon. Kodeissa voi olla viihdelaitteita, jotka voitaisiin liittää langattomaan lähiverkkoon ja näin ollen helpottaa ja mahdollistaa johdottoman tulostuksen, digiboksien päivityksen ja nauhoitettavien ohjelmien siirron tietokoneelle. [1, 277–278]

Langaton lähiverkko muodostuu yhdestä tai useasta dataa välittävästä tukiasemasta. Tukiasemat voivat olla toisissaan kytkettyinä verkkokaapelilla tai langattomasti. Tukiasemiin yhdistyvät langattomat laitteet, esimerkiksi WLAN-verkkokortti tai sovitin (kuva 1).

Kuva 1. Tukiasemat ovat kytkettyinä toisiinsa verkkokaapelilla ja langattomasti.

Langaton lähiverkko tuo hyötyjä kuin haittojakin verrattuna kiinteään verkkoon, joita ovat esimerkiksi:

- Halpa hinta. Runkoverkon ja virransyötön lisäksi ei tarvita kuin tukiasemia ja WLAN-verkkokortit. Näin se on edullinen ratkaisu yrityksille, kouluille ja terveydenhuollolle. Langattomat laitteet kuitenkin toimivat epävarmasti keskenään.
- Mobiilius. Nykypäivänä mobiililaitteiden käyttö on yleistä julkisilla alueilla, työpaikoilla, koulussa jne. WLAN:in avulla voi tarkistaa sähköpostin, jos on pääsy verkkoon. Suojaus on kuitenkin riittämätön käytettäessä WEP-salausprotokollaa mobiililaitteissa.

- Nopea käyttöönotto. Kiinteää verkkoa voidaan nopeasti ja yksinkertaisesti laajentaa kytkemällä tukiasema verkkoon. Kaikkia tietoturva-asetuksia ei välttämättä tule laitetuksi ensimmäisellä kerralla.
- Liikkuvuus. Se helpottaa laitteen siirtämistä esimerkiksi työpaikalla työpisteestä kokoushuoneeseen tai koulussa luokkahuoneesta toiseen, jolloin ei tarvitse olla sidottuna yhteen paikkaan, vaan voi liikkua vapaasti tukiaseman signaalin kantaman alueella. Intranetin käyttö langattomassa verkossa lisää kuitenkin tietoturvan riskiä.
- Nopeus. Uusi 802.11n-standardi toi mahdollisena nopeat WLAN-yhteydet, jolloin mukavuus lisääntyy käytettäessä Internetiä. Signaalin kantomatka tukiasemasta on rajattu, jolloin Internet-yhteys kuitenkin hidastuu kauemmaksi mentäessä. [1, 280]

WLAN-verkkoja hyödynnetään useissa eri paikoissa ja yrityksissä. Kämmenlukijoita varastovalvonnassa käytettäessä yritys voi pitää itseään ajan tasalla valvomalla varastosaldoaan ja keräämällä tietoa, joka taas parantaa tehokkuutta ja tarkkuutta. Tiedot menevät siis suoraan pääkoneelle, jolloin paperityötä ei tarvita ja inhimilliset erehdykset pienenevät.

Lukioissa ja ammattikouluissa voisi olla oppilaille tarjolla langaton verkko, johon he voisivat liittyä oman langattoman laitteensa kanssa. Jos tietokoneluokat ovat täynnä tai suljettuina, voisivat he käyttää omaa langatonta laitettaan esimerkiksi tiedon etsimiseen Internetistä.

Sähkölaitoksissa automaattinen mittarinlukeminen hoidetaan etäseurantana langattomasti, jolloin ei tarvitse käydä lukemassa tuloksia, kirjoittaa tuloksia paperille ja kirjata niitä tietokoneelle. Langattomuus mahdollistaa tietojen lähettämisen automaattisesti sähkölaitokselle tietyin väliajoin. Tämä säästää huomattavasti aikaa ja pienentää kustannuksia. [2, 17–20]

Tekniikan kehittyessä langattomuus tuo paljon uusia mahdollisuuksia kotona käytettäväksi. Televisiot voidaan kytkeä langattomasti, jolloin pystytään käyttämään Internet-palveluita. Musiikin kuuntelu, kuvien-, ja elokuvien katselu verkon yli on myös mahdollista.

3 LANGATTOMAN VERKON STANDARDIT

IEEE (Institute of Electrical and Electronics Engineers) 802.11 -standardi määrittelee WLAN-verkoille MACin (Media Access Control) ja useita fyysisiä kerroksia. Ensimmäinen 802.11-standardi julkaistiin vuonna 1997, mutta langattomat lähiverkot yleistyivät paremmin vasta vuonna 2001, jolloin hinnat putosivat. IEEE 802.11 -standardille on määrätty oma työryhmä, joka kehittää langattomien lähiverkkojen suorituskykyä ja tietoturvaa entistä paremmaksi.

Standardi määrittelee useita asioita, esimerkiksi MAC-kerroksen, skannauksen ja todennuksen. Standardi määrittää MAC-kerroksen, joka tarjoaa useita 802.11-pohjaisten langattomien lähiverkon toimintaa tukevia toimintoja. Skannaus määrittelee passiivisuuden tai aktiivisuuden, jossa radioverkkokortti etsii tukiasemia. Todennus määrittelee kaksi muotoa, avoimen todennuksen ja jaetun avaimen todennuksen. Taulukosta 1 nähdään yhteenveto 802.11-standardien ominaisuuksista. [2, 118]

Standardi	Julkaisuvuosi	Taajuus	Huippunopeus
802.11a	1999	5 GHz	54 Mbit/s
802.11b	1999	2,4 GHz	11 Mbit/s
802.11g	2003	2,4 GHz	54 Mbit/s
802.11n	Ei tiedossa	2,4 ja 5 GHz	600 Mbit/s

Taulukko 1. IEEE 802.11 -standardien yhteenveto, jossa on vuosi, taajuus ja nopeus.

3.1 802.11a

802.11a julkaistiin vuoden 1999 lopussa. Se käyttää 5 GHz:n taajuutta käyttäen OFDM (Orthogonal Frequency Division Multiplexing) -tekniikkaa. Huippunopeus on 54 Mbit/s, mutta realistinen nopeus jää kuitenkin 20–25 Mbit/s:n paikkeille. 802.11a-standardi pystyy toimimaan usealla ei-päällekkäisellä kanavalla. Se pystyy myös säätämään erilaisia bittinopeuksia, kuten 6, 9, 12, 18, 24, 48 tai 54 Mbit/s. Signaalin kantavuus on noin 30 metriä riippuen todellisesta tiedonsiirtonopeudesta.

Vasta vuoden 2001 loppupuolella 802.11a-tukiasemat ja verkkokortit tulivat markkinoille. Tämän vuoksi sen asennuskanta on jäänyt pieneksi verrattuna 802.11b:en. Etuna on suurin kapasiteetti, koska se toimii usealla ei-päällekkäisellä kanavalla. 5 GHz:n taajuudella ei ole niin paljon häiriötekijöitä kuin 2,4 GHz:llä. Tämä tekee siitä varteen otettavan ehdokkaan. 802.11a ei ole yhteensopiva muiden 802.11b/g/n standardien kanssa. [2, 124], [3]

3.2 802.11b

802.11b-standardi tehtiin samanaikaisesti 802.11a:n kanssa, mutta se julkaistiin paria kuukautta aiemmin samana vuonna 1999 kuin 802.11a-standardi. Kyseisen standardin tukiasemia ja verkkokortteja on ollut saatavilla jo vuodesta 1999. Siksi useimmat käytössä olevat langattomat lähiverkot ovat yhteensopivia.

802.11b käyttää 2,4 GHz:n taajuutta, jossa on kolme ei-päällekkäistä kanavaa ja ongelmana ovat muiden samaa taajuutta käyttävien radiolaitteiden häiriöt. Huippunopeus on 11 Mbit/s, mutta se pystyy säätämään bittinopeuttaan 1, 2, 5,5 tai 11 Mbit/s. Realistinen tiedonsiirtonopeus on noin puolet maksimista eli 5–6 Mbit/s. Signaalin kantavuus voi olla sisällä korkeintaan 100 metriä. [2, 126–127], [3], [4, 34],

3.3 802.11g

Vuonna 2003 julkaistiin uusi 802.11g-standardi, joka toi mukanaan paremman tietoturvan. Se toimii 2,4 GHz:n taajuudella käyttäen OFDM-tekniikkaa. Huippunopeus on 54 Mbit/s mutta realistinen tiedonsiirto jää kuitenkin noin 20 Mbit/s, joten voi jäädä alle 802.11a-standardin nopeuden. 802.11g pystyy säätämään bittinopeuttaan 6, 9, 12, 18, 24, 36, 48 tai 54 Mbit/s.

802.11g-standardin ongelmina ovat kolme ei-päällekkäistä kanavaa ja muiden samaa taajuutta käyttävien radiolaitteiden aiheuttamat häiriöt. 802.11g on alaspäin yhteensopiva 802.11b-standardin kanssa. 802.11g:stä tuli kilpaileva standardi 802.11a kanssa. Sisällä signaalin kantavuus on noin 50 metriä ja ulkona 100 metriä. [2, 127], [3]

3.4 802.11n

802.11g-standardin jälkeen tuli 802.11n-standardi. Se tukee 2,4 GHz:n ja 5 GHz:n taajuuksia, joten se on alaspäin yhteensopiva aikaisempien standardien kanssa. 802.11n-standardissa luvataan jopa 600 Mbit/s tiedonsiirron nopeutta, mutta se jää alle kolmanneksen luvatusta.

802.11n-standardi tuo mukanaan MIMO (Multiple Input Multiple Output) -tekniikan, joka hyödyntää monitie-etenemistä, jossa signaalit kimpoilevat seinien, ovien ja muiden esineiden kautta vastaanottimen antenniin. Kyseisen tekniikan avulla saadaan nopeudet suuremmiksi käyttämällä jopa neljää antennia ja useita kanavia samaan aikaan. [5]

3.5 802.11x

802.11x-standardin käyttö antaa toimivat puitteet suojattuun langattomaan verkkoon, käyttäjäliikenteen todennukseen ja valvontaan. Se tarjoaa myös tietyin väliajoin muuttuvan salausavaimen. Standardi yhdistää EAP (Extensible Authentication Protocol) -protokollan käytön ja tukee monia eri todennusmenetelmiä. Tämä tarjoaa tehokkaan todennuksen riippumatta siitä, mitä suojausmetodia käytetään tai onko suojausta ollenkaan.

802.11x-liikenne lähtee käyntiin, kun tuntematon langaton laite yrittää muodostaa yhteyttä tukiasemaan. Portin avaamalla tukiasema vastaa pyyntöön, jossa hyväksytään ainoastaan EAP-paketit käyttäjältä palvelimelle. Kaikki muu liikenne on estettyä, kuten HTTP (Hypertext Transfer Protocol) ja DHCP (Dynamic Host Configuration Protocol), kunnes tukiasema pystyy tunnistamaan käyttäjän palvelimelta. Kun käyttäjä on saatu tunnistettua palvelimelta, tukiasema avaa portin myös toisenlaiseen verkkoliikenteeseen käyttäjän oikeuksien mukaan. [2, 188–190]

Käyttäjän tunnistamiseen käytetään useimmiten RADIUS (Remote Authentication Dial In User Service) -palvelinta, joka hoitaa tunnistuksen. Se antaa käyttäjälle luvan verkon voimavaroihin ja pitää yllä verkonhallinnassa tarvittavia tietokantoja. AAA (Authentication, Authorization and Accounting) -protokolla tai -palvelin on usein palvelimista ja niiden käyttämistä protokollista käytettävä nimitys. [6, 297–298]

4 LANGATTOMAN VERKON SALAUSPROTOKOLLAT

Ilman salausprotokollaa jokainen voisi käyttää kenen tahansa langatonta lähiverkkoa ja päästä käsiksi langattomassa verkossa liikkuvaan tietoliikenteeseen. Toisin sanoen käyttäjä avaa tietokoneensa ja verkkonsa avoimeksi esimerkiksi siitä hyötyville hakkereille. Salauksen ideana on salata tietoliikenteen tietoja tukiaseman ja langattoman laitteen välillä muuntamalla datapaketin bittejä, jolloin salakuuntelijoiden datan purkaminen vaikeutuu. Taulukosta 2 nähdään salausprotokollien yhteenveto. [2, 178]

Salausprotokolla	Salaus	Salausavaimen pituus	Salausalgoritmi
WEP	-	64- ja 128-bittiä	RC4
WPA	TKIP	128-bittiä	RC4
WPA2	AES	128-, 196- ja 256-bittiä	Rijndael

Taulukko 2. Salausprotokollien yhteenveto, jossa on tiedot tiivistettynä.

4.1 WEP

802.11-standardi sisälsi WEP-salauksen, jossa alussa käytettiin 40-bittistä jaettua avainta, joka todettiin standardointiaikaan riittämättömäksi suojaukseksi. Myöhemmin salausavainta kasvatettiin 104 bittiin, mikä ei olekaan riittävä suojaus. WEP-salausprotokolla käyttää RC4-jonosalausta, jossa avaimen täytyy olla samanpituinen kuin käytettävä ja salattava tavujono [4, 79–80]. Salausavaimien pituudet ovat 64- ja 128-bittinen, joista alustusvektori on 24 bittiä. WEP:ssä on useita heikkouksia, mutta tässä ovat kolme oleellisinta:

- 24-bittinen alustusvektorin numeerinen rajoittuneisuus, josta seuraa arvojen ja avaimien toistuminen ennen pitkään, jolloin murtautujat pystyvät murtamaan WEP-avaimen.
- 16 miljoonasta kaikkia arvoja ei voida käyttää, kuten numero 1. Se ei ole täysin käyttökelpoinen, koska murtautuja voi käyttää heikkojen alustusvektori arvojen käyttämiseen työkalua, jolloin saadaan murrettua WEP.

- 64- ja 128-bittisen salausavaimen erot eivät ole suuret, vaikka niin voisi kuvitella. Molemmat käyttävät samaa 24-bittistä alustusvektoria, jossa on omat heikkoutensa. Toisin sanoen 128-bittinen salaus ei ole sen turvallisempi langattoman verkon tietoturvaa ajatellen kuin 64-bittinen salaus. [1, 306]

4.2 WPA

WPA-suojaus oli päivitys WEP-salausprotokollaan, joka toi dynaamisen avaimen salauksen ja kaksisuuntaisen todennuksen. Käyttäjän ja langattoman verkon täytyy tunnistaa toisensa nelivaiheisessa kättelyssä. Se toi uutuutena TKIP (Temporal Key Integrity Protocol) -salauksen, joka vaihtaa väliaikaisia avaimia lakkaamatta 10 000 paketin välein.

WPA-salausavaimen pituus on 128-bittiä per paketti ja joka kerta luo dynaamisesti uuden avaimen jokaiselle paketille estäen näin törmäykset. WPA käyttää liikenteen salaamiseen samaa kuin WEP eli RC4-algoritmia. [2, 183–184]

4.3 WPA2

WPA2 on päivitys edelliseen WPA-salausprotokollaan. Kyseinen suojausmenetelmä on uusin ja turvallisin. WPA2 toi AES (Advenced Encryption Standard) -salauksen, mikä on turvallisempi. AES ei käytä enää RC4-salausalgoritmia vaan sen korvasi Rijndael-algoritmi, joka on vahvempi.

WPA2 kykenee käyttämään eripituisia salausavaimia, jonka vaihtoehtoina ovat 128, 196 ja 256-bittiset. Suurin osa tutkijoista on sitä mieltä, että AES-salaus ei ole murrettavissa. [2, 184], [4, 84]

5 LANGATTOMAN VERKON TIETOTURVA

WLAN-verkkoihin kohdistuvat uhat ovat useimmiten samoja kuin kiinteässä verkossa. Langattomuuden myötä on tullut uusia murtautumismenetelmiä. Erilaisia tietoturvauhkia on useita, esimerkiksi passiivinen tarkkailu ja palvelunesto ja tulee lisää koko ajan. Hakkerit voivat tunkeutua langattomaan verkkoon, varastaa yrityksen tietoja ja aiheuttaa ongelmia. Naapuri voi käyttää toisen naapurin langatonta verkkoa ja siepata mahdollisesti tärkeää tietoa. [2, 171], [4, 69]

5.1 Passiiviset uhat

Vakavista passiivisista langattoman verkon uhkista on liikenteen salakuuntelu, joka voidaan tehdä myös rakennuksen ulkopuolelta. Siinä tarkoituksena on kerätä tietoa, joka auttaa verkkoon murtautumisessa. Salakuuntelua on vaikea estää ja mahdoton havaita.

Liikenteen analysointi, jolloin luottamukselliset tiedot voi paljastua verkon dataliikenteessä. Jälkeenpäin tietoa on mahdollista tutkia. Salakuunteluun ja tutkimiseen on saatavilla erilaisia ohjelmia, kuten esimerkiksi Ettercap-ng.

Välistävetohyökkäys, jonka tarkoituksena on laatia valelaite käyttäjän ja tukiaseman väliin. Yleisin tapa hyökkäyksissä on käyttää ARP (Address Resolution Protocol) -protokollaa. Murtautuja pystyy ottamaan verkon hallintaansa oikeilla välineillä. [2, 174], [4, 69]

5.2 Aktiiviset uhat

Aktiivisissa uhkissa lähetetään langattomaan verkkoon dataa tai signaaleja. Signaalien häirintä, joka voidaan toteuttaa radiolähettimellä tai ylikuormittamalla tukiasemia tai muita laitteita turhilla yhdistämis- tai palvelupyynnöillä. Signaalien häirintään voi valmistautua, esimerkiksi pitämällä verkko erossa vierailta häiriöiltä.

WLAN-verkossa dataliikenteen muokkaaminen tapahtuu harkitusti tai tahattomasti. Harkittu muokkaus perustuu useimmiten välistävetohyökkäykseen. Tahattomasti

turmeltu data havaitaan tarkistussummasta ja näin ollen se hylätään virheellisenä. Tiedon muokkaaminen voidaan havaita oikeilla menetelmillä.

Hakkereiden tavoite on tietojärjestelmiin tunkeutuminen ja päästääkseen tavoitteeseen he käyttävät mitä tahansa keinoja Kun yrityksessä käytetään langatonta verkkoa, voi murtautuja hyödyntää yrityksen sisäisiä palvelimia ja työasemia. Palvelimet ovat usein vahvasti ja ammattimaisesti suojattuja, mutta työasemien tietoturvat voivat silti olla huonosti hoidettuja. Palvelimiin tehdyt murtautumisyritykset huomataan yleensä, mutta työasemiin murtautumista ei huomata yhtä hyvin. [4, 69],

Palvelunestohyökkäys, jonka muotoja on erilaisia, esimerkiksi väsytyshyökkäys, jossa langattomaan verkkoon lähetetään iso määrä paketteja. Kun saadaan verkkoliikenne kuluttamaan kaikki voimavarat, langaton verkko kaatuu. Toinen vaihtoehto on pysäyttää WLAN-verkot käyttäen tehokasta signaalia, joka häiritsee WLAN-laitteita. Silloin tehokkaampi signaali hallitsee etenemistä ja saa tukiasemat ja WLAN-verkkokortit hyödyttömiksi. Taulukosta 3 nähdään yhteenvetona passiiviset sekä aktiiviset uhat. [2, 176]

Passiiviset uhat	Aktiiviset uhat
Liikenteen salakuuntelu	Langattoman verkon häirintä
Liikenteen analysointi	Dataliikenteen muokkaaminen
Välistävetohyökkäys	Palvelusestohyökkäys

Taulukko 3. Uhkien yhteenveto, jossa luetellaan passiivisia ja aktiivisia uhkia.

5.3 SSID

SSID (Service Set Identifier) on WLAN-verkon nimi, jolla erotetaan WLAN-verkot toisistaan. Nimen täytyy olla sama kaikilla laitteilla, jotta ne voivat viestiä keskenään, ja pituus saa olla enintään 32 merkkiä [7, 413]. Langattoman verkon nimenä on yleensä tukiasemassa laitevalmistajan tai verkkopalvelun tarjoajan nimi oletuksena. Se vaihtamista suositellaan, ellei halua mainostaa tai edesauttaa verkkoon murtautumista.

Verkon tunnuksen lähetyksen voi myös ottaa pois päältä, jolloin se ei näy kuuluvuusalueella olevien päätelaitteiden verkkoluettelossa. Ennen tämä oli

tietoturvamielessä suositeltavaa tehdä, koska antoi paremman turvan. Joidenkin verkkopäätteiden valmistajien laitteet näyttävät verkkoluettelossa, ettei SSID tunnusta lähetetä, jos se on pois kytkettynä päältä. Se ei siis tuo minkäänlaista turvaa eli on sama, piilottaako verkon nimen vai antaako sen näkyä. Enemmän työtä aiheutuu langattomaan verkkoon kytkeytymisessä, jos verkon nimen lähetys on poissa päältä.

5.4 Tietoturvan parantaminen

WLAN-verkkojen turvallisuutta voidaan parantaa yksinkertaisilla perusasioilla. WEP-, WPA- ja WPA2-salausprotokollia pystytään parantamaan RADIUS (Remote Authentication Dial In User Service) -palvelimella, mutta on epätodennäköistä, että sellaista olisi monella, varsinkaan kotikäyttäjillä. Oikeanlaisen tietoturvan toteuttaminen vaatii perehtymistä asiaan ja hyvää suunnittelua. Seuraavana tietoturvan parantamisen ehdotuksia:

- Suojataan tukiasema fyysisesti sijoittamalla asema ulkopuolisten ja käyttäjien läheltä pois.
- Langattoman verkon nimen eli SSID:n vaihtaminen ja verkon piilottaminen.
- Standardin 802.11x:n käyttäminen käyttäjien oikeuksienhallinnassa ja todennuksessa.
- Yhteyden aikakatkaisun oletusarvo muutetaan maksimissaan kymmeneen minuuttiin.
- Sallitaan etähallinnan käyttöön ainoastaan salattuja yhteyksiä ja määrätyistä IP-osoitteista.
- Tutustuminen EAP-protokolliin (Extensible Authentication Protocol) ja itselle parhaan vaihtoehdon valitseminen. [1, 311–312], [4, 71]

6 TUTKIMUSYMPÄRISTÖN SUUNNITTELU

WEP-, WPA- ja WPA2-salausprotokolliin hyökätessä käytetään menetelmiä välistäveto ja sanakirja. Välistävetohyökkäystä eli Man in the Middleä käytetään WEP-salausavaimen murtamiseen. Hyökkäyksessä seurataan käyttäjän ja tukiaseman dataliikennettä. Dataliikenteestä saadaan siepattua viestejä, joita lähetetään langattomaan verkkoon takaisin. Näin ollen tukiasemaa saadaan huijattua ja uskomaan, että hyväksytty käyttäjä lähettää viestit. Tämä toteutetaan siten, että siepataan ARP-viestejä (Address Resolution Protocol), joita lähettämällä voidaan jopa nelinkertaistaa alustusvektoreiden sieppausnopeus. Kun alustusvektoreita on siepattu tarpeeksi, pystytään murtamaan WEP-salausavain.

Sanakirja- eli Dictionary Brute Force-hyökkäysmenetelmää käytetään molempia WPA- ja WPA2-salausavaimia vastaan. Tarkoituksena on verrata salausavainta sanakirjatiedostossa oleviin sanoihin ja numeroihin. Kyseiseen sanakirjatiedostoon on kirjattu erilaisia sanoja. Erilaisia ja monipuolisempia sanakirjalistoja on saatavilla Internetistä. Tiedostossa olevat sanat ja numerot voi olla otettu mistä vaan ja kirjattu sekaisin tiedostoon. Käytetyt sanat koostuvat yleensä etu- ja sukunimistä sekä paikannimistä. Salasanan vertaamisen nopeus sanoihin riippuu tietokoneen prosessorin tehosta ja sanakirjan tiedoston koosta.

6.1 Laitteisto

Tutkimuslaitteistoon kuuluvat ZyXel Prestige 660HW-D1 ADLS2+ -tukiasema, Acer Aspire 7730G kannettavan tietokoneen sisäinen WLAN-verkkokortti Intel(R) WiFi Link 5100 AGN sekä kaksi minikannettavaa, joissa käyttöjärjestelminä ovat Windows XP ja 7 (kuva 2).

Kuva 2. Tutkimuslaitteisto, johon kuuluu tukiasema ja kaksi minikannettavaa.

Zyxel Prestige tukiasema tukee 802.11b/g standardeja sekä WEP-, WPA- ja WPA2-salausprotokollia. Tutkimuksessa käytetään 802.11g-standardia ja kyseisiä salausprotokollia, joten tukiasema sopii tähän. Salauksien purkamisessa ja langattomien verkkojen etsinnöissä käytetään Acer Aspire 7730G kannettavan tietokoneen sisäistä WLAN-verkkokorttia Intel(R) WiFi Link 5100 AGN. Kannettavan tietokoneen WLAN-verkkokortti tukee 802.11a/b/g/n-standardeja. Verkkokortissa ei käytetä normaaleja ajureita vaan muokattuja ajureita. Tutkimuksissa on mukana myös kaksi minikannettavaa. Niissä on eri käyttöjärjestelmät, jolloin nähdään, onko tietokoneen käyttöjärjestelmällä merkitystä suojausta ajatellen.

6.2 Salausavaimen purkaminen

Salausavaimen purkaminen tehdään kannettavalla tietokoneella, jossa on Linux Ubuntu-käyttöjärjestelmä. Siihen asennetaan aircrack-ng-murto-ohjelmisto. Tähän olisi sopinut hyvin BackTrack-ohjelmisto, joka on myös Linux-pohjainen.

Kyseisellä aircrack-ng-murtautumisohjelmistolla tehdään seuraavat toimenpiteet:

- pakettilähettämisen toimivuuden testaus
- langattomien lähiverkkojen etsintä ja datansieppaus
- hyökkäykset WEP-salausprotokollan langattomaan verkkoon
- hyökkäykset WPA- ja WPA2-salausprotokollan langattomaan verkkoon.

7 SALATUN VERKKOLIIKENTEEN PURKAMINEN

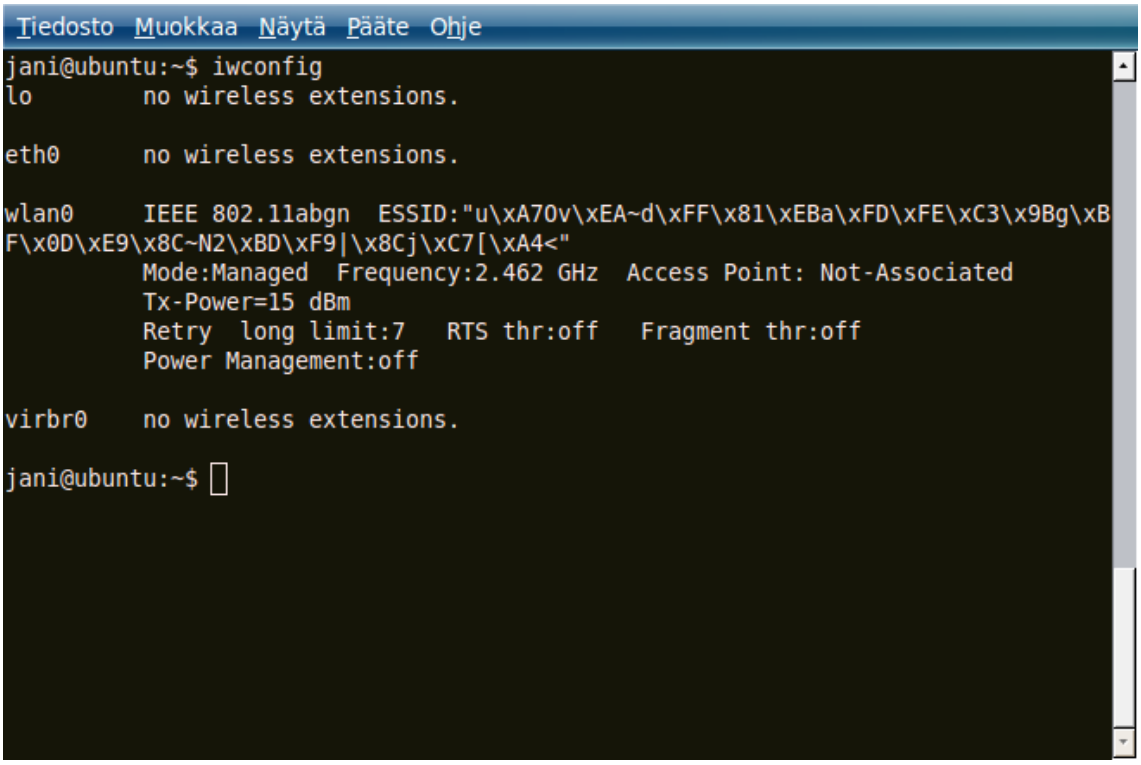
Verkkoliikenteen purkamisen ensimmäinen vaihe on asentaa aircrack-ng-ohjelmisto avaamalla pääteikkuna. Jos ei ole kirjautunut Linux-järjestelmän pääkäyttäjänä sisälle, pitää komennon eteen kirjoittaa ”sudo” (komento 1).

```
sudo apt-get install aircrack-ng                    (1)
```

Seuraavaksi on syytä tarkistaa, onko aircrack-ng-ohjelmisto löytänyt WLAN-verkkokortin itse vai täytyykö verkkokortin ajurit asentaa manuaalisesti. Tämä tapahtuu avaamalla pääteikkuna, jossa syötetään komento (komento 2).

```
iwconfig                                            (2)
```

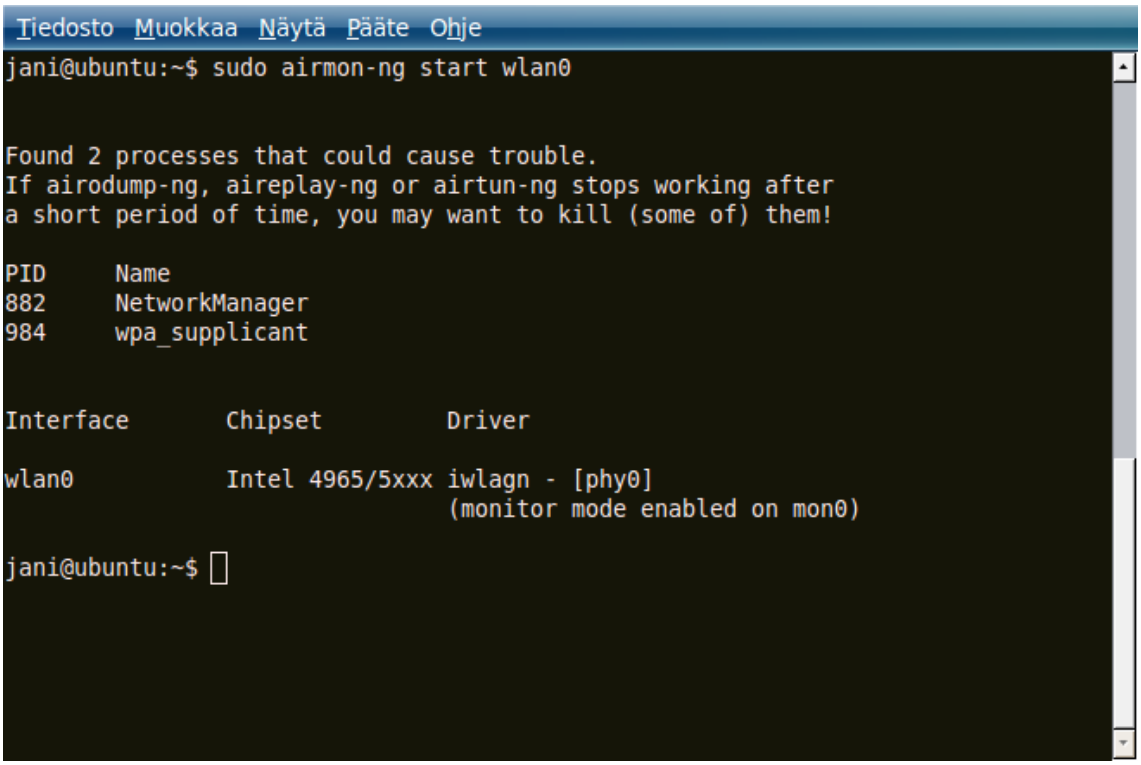
WLAN-verkkokortti Intel(R) WiFi Link 5100 AGN pitäisi näkyä päätteellä “wlan0” nimisenä, koska sisäinen verkkokortti löytyy (kuva 3). Jos aircrak-ng-ohjelmisto ei tunnista korttia, ajurit täytyy asentaa manuaalisesti. Ajureiden kanssa pitää olla tarkkana, että ne ovat yhteensopivia kernelin eli ytimen kanssa.



Kuva 3. WLAN-verkkokortti löytyy, joten ajureita ei tarvitse asentaa.

WLAN-verkkokortin löytämisen tai ajureiden asentamisen jälkeen on vuorossa WLAN-verkkokortin monitor mode -tilaan saaminen (kuva 4). Tällä tavoin saadaan siepattua paketteja ilman yhdistymistä tukiasemaan [8]. Verkkokortti laitetaan kyseiseen monitor mode -tilaan ”mon0” (komento 3).

```
sudo airmon-ng start wlan0
```
(3)



Kuva 4. WLAN-verkkokortti on kytketty monitor mode -tilaan.

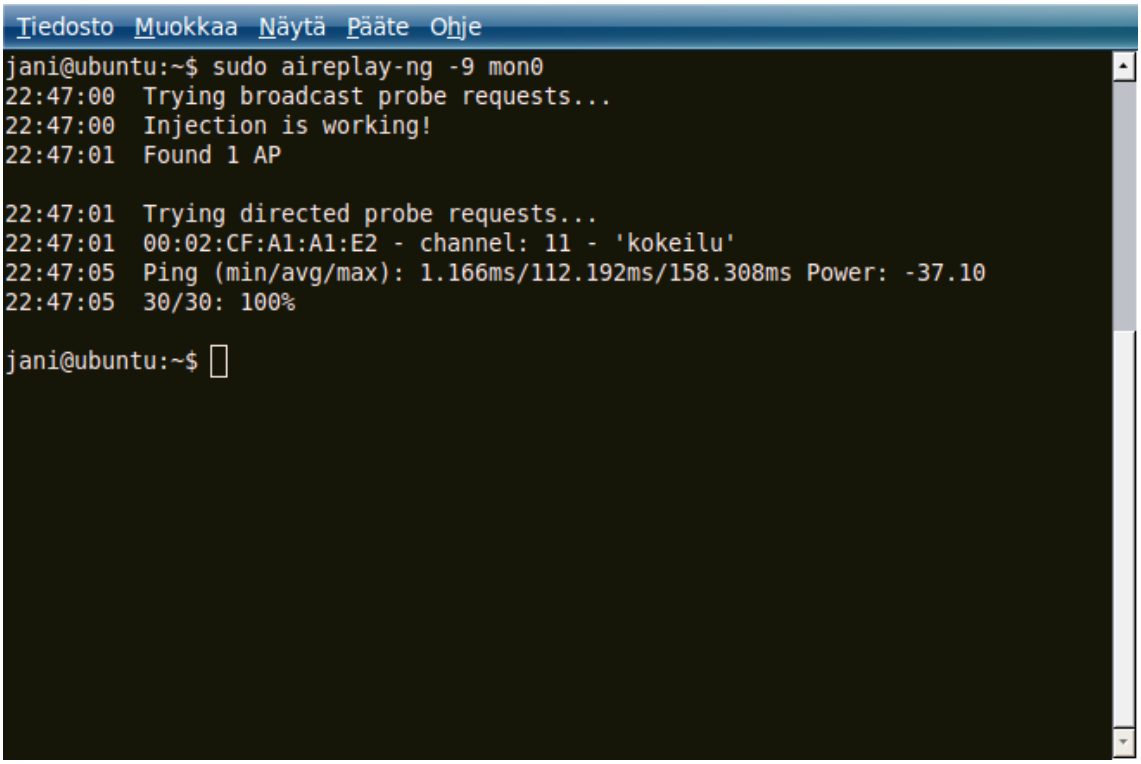
Muokatut WLAN-verkkokortin ajurit eroavat siten normaaleista, että ne mahdollistavat kytkeytymisen monitor mode -tilaan ja lähettävät paketteja langattomaan verkkoon [9]. Aireplay-ng on aircrack-ng-murtamisohjelmiston mukana tuleva ohjelma, jolla voidaan tehdä monia erilaisia hyökkäyksiä langattomaan verkkoon.

Seuraavaksi tehdään automaattinen kokeilutoiminto, jossa kokeillaan ja varmistetaan pakettilähettämisen toimivuutta (komento 4).

```
sudo aireplay-ng -9 mon0
```
(4)

Sen tarkoituksena on etsiä tukiasema ja kokeilla pakettien lähettämistä. Paketteja lähetettiin kaikkiaan 30, joista kaikki saatiin menemään perille niin kuin kuvassa 5

voidaan nähdä. Näin ollen kokeilu osoitti, että verkkokortin muokatut ajurit toimivat ja tukevat paketinlähettämistä. Kaikki tarpeellinen on kunnossa ja voidaan edetä WEP-salausavaimen murtamiseen.



Kuva 5. Packet injection -kokeilu on suoriutunut onnistuneesti.

7.1 Langattomien verkkojen etsintä ja tiedon keräys

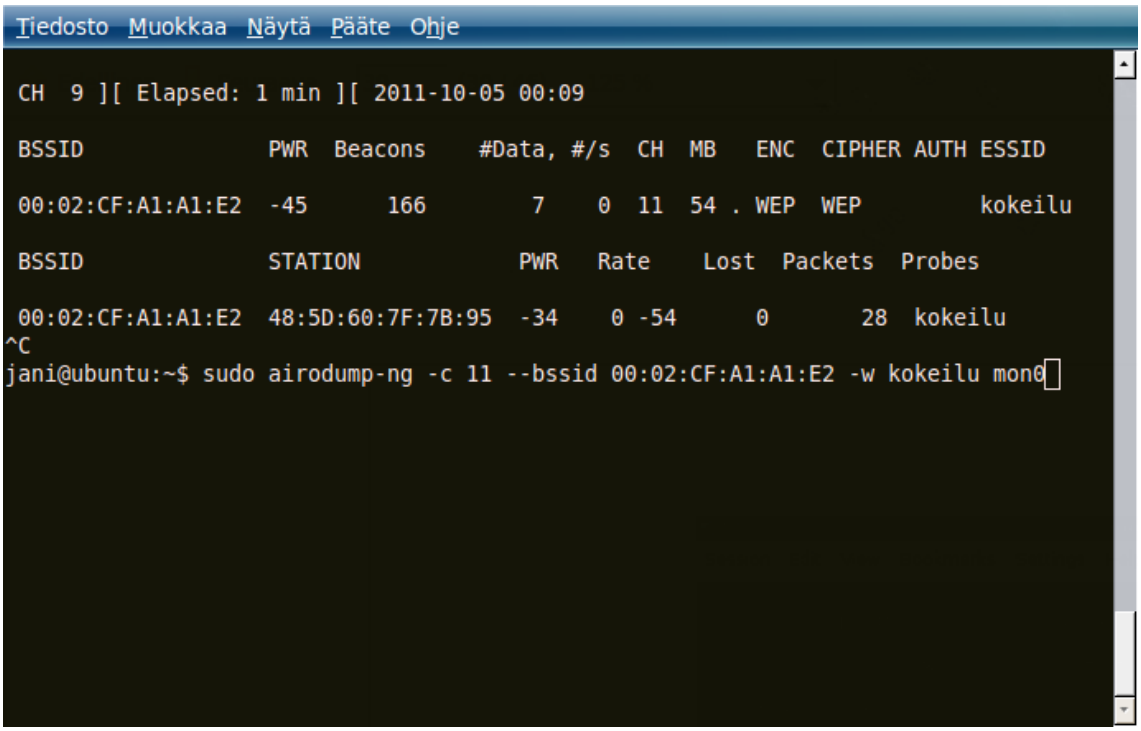
Seuraavana täytyy etsiä tukiasema ja ryhtyä keräämään tietoa langattomasta verkosta (komento 5). Tähän löytyy aircrack-ng-murtautumisohjelmistosta airodump-ng, joka on tarkoitettu tiedonkeräykseen [10]. Ohjelmaa voidaan käyttää, vaikka olisi WEP-, WPA- tai WPA2-salausprotokolla käytössä.

```
sudo airodump-ng mon0                                    (5)
```

WLAN-verkkokortti aloittaa tiedonkeräämisen signaalin kantaman alueelta löytyvistä tukiasemista ja kaikilta kanavilta. Kaikista löytyneistä tukiasemista on turha kerätä tietoa. Tiedonkeräys kannattaa kohdistaa haluttuun tukiasemaan, jolloin säästytään ylimääräiseltä tiedonkeräykseltä. Kun kohdistetaan tiedonkeräys haluttuun tukiasemaan, käynnistetään airodump-ng-ohjelma uudelleen (komento 6).

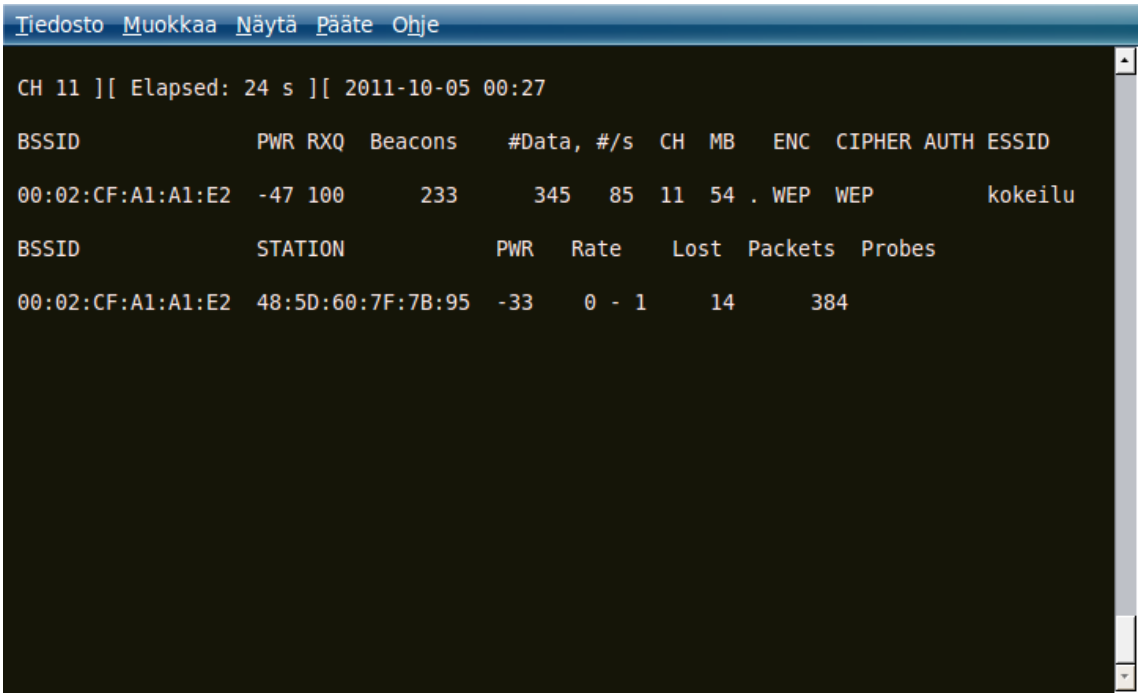
```
sudo airodump-ng -c 11 --bssid 00:02:CF:A1:A1:E2 -w kokeilu mon0        (6)
```

Kuvassa 6 on annettu kanava, jolta tietoa kerätään ja tukiaseman MAC-osoite, johon keräys kohdistetaan. Tallennettavat tiedostot nimetään kokeiluksi.



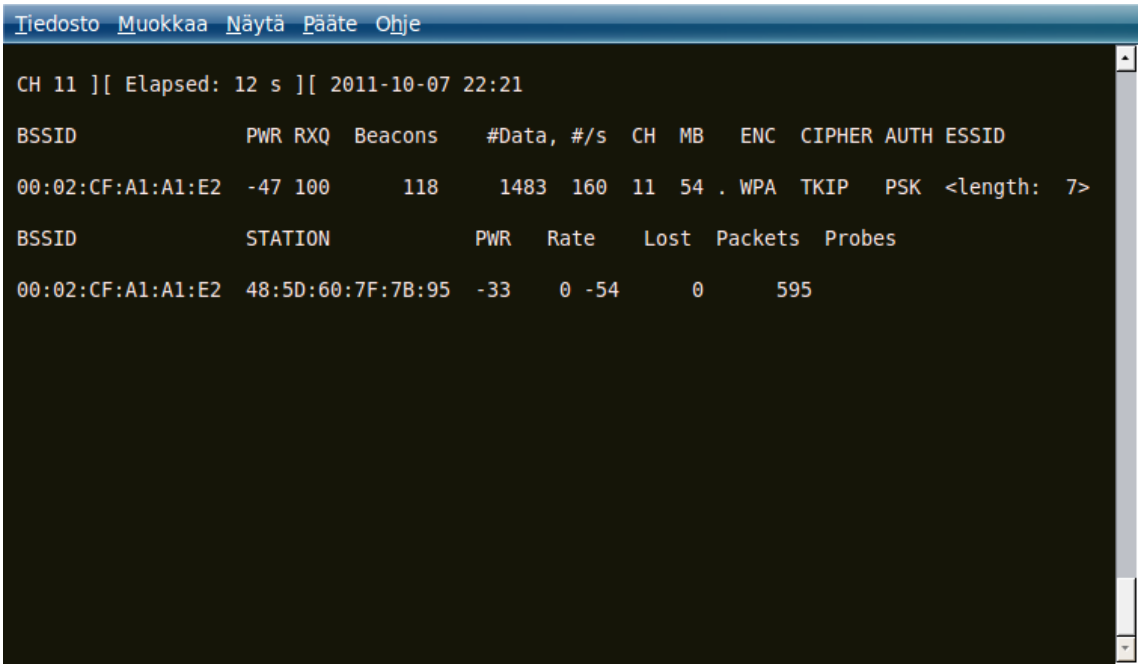
Kuva 6. Airodump-ng-ohjelmaa tarkennetaan haluttuun tukiasemaan.

Tarkemmin kohdistetussa tukiaseman tiedon keräämisessä airodump-ng-ohjelma näyttää kohdistetun tukiaseman ja yhdistyneet käyttäjät, kun niitä löytyy. Kyseinen ohjelma kertoo monipuolista tietoa langattomista verkoista, kuten esimerkiksi tukiaseman MAC-osoitteen, siepatut datapaketit, kanavan, salausprotokollan ja verkon nimen (kuva 7).



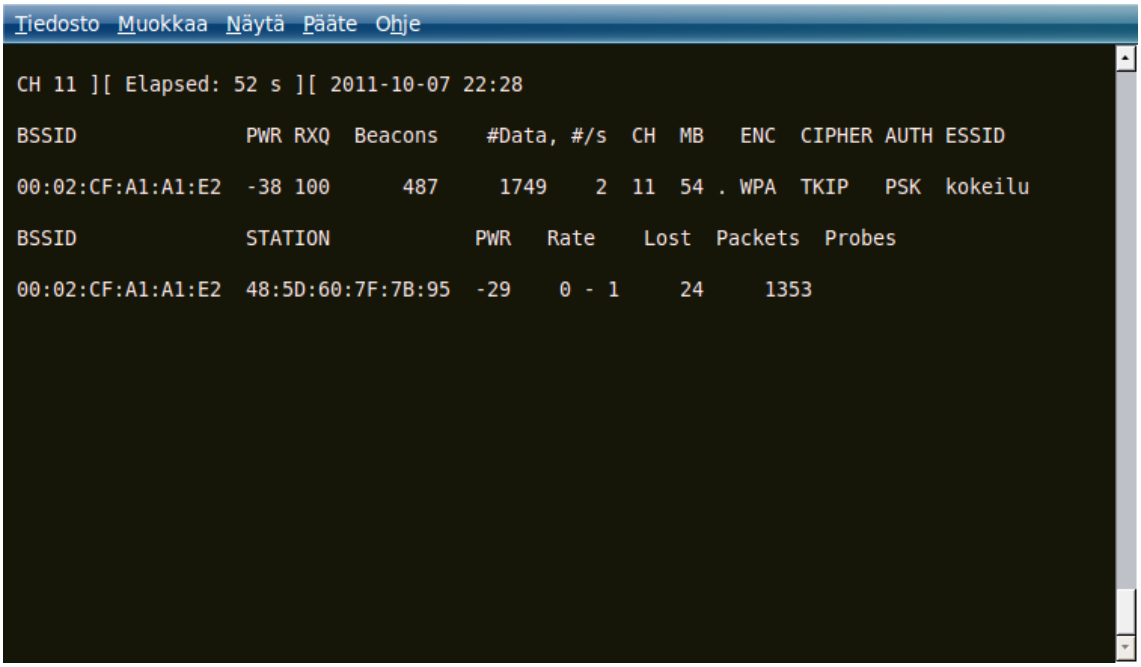
Kuva 7. Airodump-ng-ohjelma on tarkennettuna haluttuun tukiasemaan.

Vaikka langattoman verkon nimen lähetys olisi kytketty poissa päältä, airodump-ng-ohjelma saa selville langattoman verkon nimen. Aluksi ”ESSID” kohdalla näkyy ”length: 7”, joka ilmaisee, että langattoman verkon nimi on piilotettu (kuva 8). Siitä tiedetään ainoastaan langattoman verkon nimen pituus, mikä ilmaistaan numeroin. Mahdollista on, että numero onkin nolla tai ykkönen, jolloin tukiasema ei paljasta nimen oikeaa pituutta. Silloin oikea pituus voi olla, mikä numero tahansa. [10]



Kuva 8. Airodump-ng-ohjelma näyttää, että langattoman verkon nimi on piilotettu.

Kun käyttäjä yhdistyy tukiasemaan, airodump-ng-ohjelma sieppaa langattoman verkon nimen ja näyttää sen (kuva 9). [10]



Kuva 9. Airodump-ng-ohjelma näyttää, että langattoman verkon nimi on selvitetty.

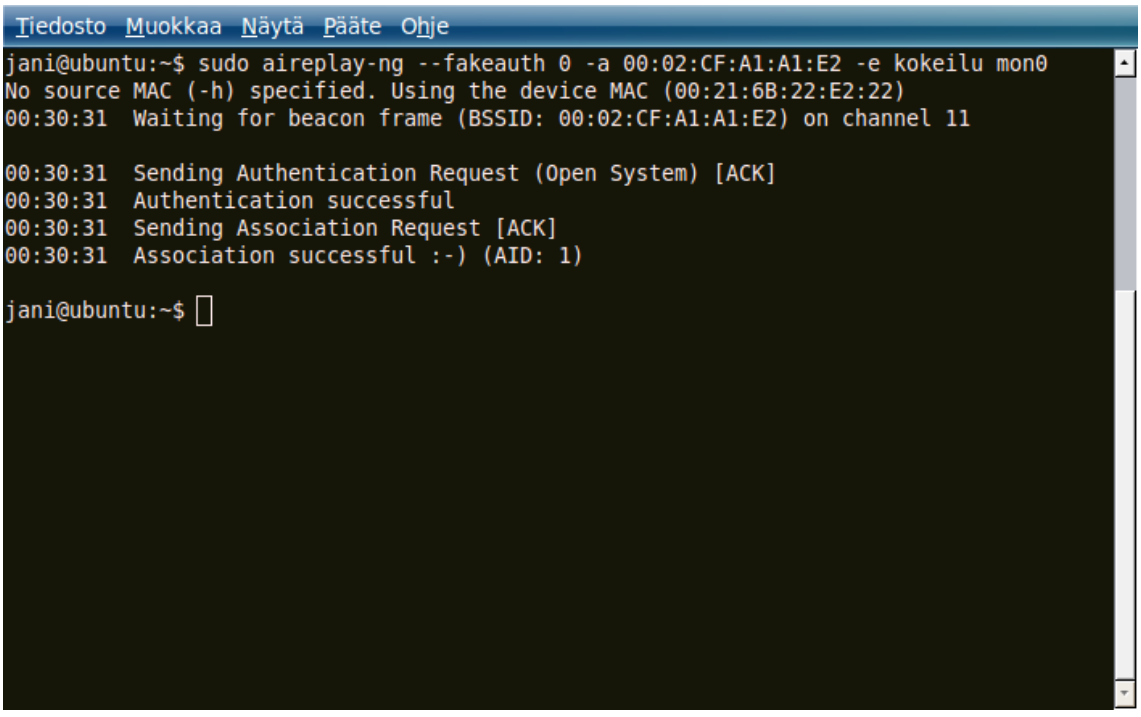
7.2 WEP-salausavaimen purku

Tässä osiossa käyttäjä on yhdistynyt valmiiksi tukiasemaan. Tukiasemaan on määritetty 64-bittinen WEP-salausavain avoimella todennuksella, jolloin tukiasema hyväksyy kaikkien langattomien laitteiden yhdistämisen itseensä. Yhdistyminen tukiasemaan ei kuitenkaan onnistu ilman kyseistä salausavainta, mutta sallii pakettien lähettämisen langattomaan verkkoon.

Tukiasemaan tehdään valeautentikointihyökkäys, jolla oma WLAN-verkkokortti saadaan yhdistettyä langattomaan verkkoon nimeltä kokeilu (komento 7), (kuva 10).

```
sudo aireplay-ng --fakeauth 0 -a 00:02:CF:A1:A1:E2 -e kokeilu mon0        (7)
```

Tämä mahdollistaa sen, että seuraavaksi siepattujen alustusvektori pakettien kasvua saadaan nopeutettua erilaisilla hyökkäyksillä. Näin saadaan lyhennettyä aikaa, joka menee WEP-salausavaimen murtamiseen. [11]

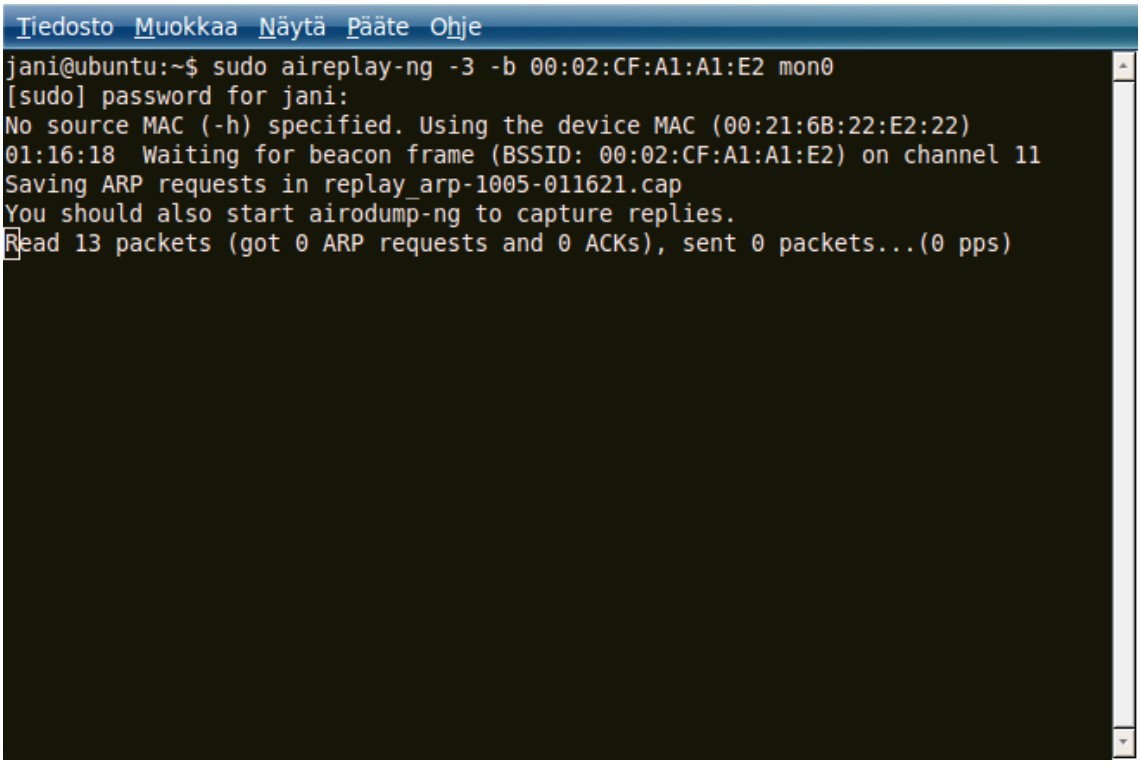


Kuva 10. Valeautentikointihyökkäys on tehty onnistuneesti tukiasemaan.

Seuraavaksi käynnistetään hyökkäys, jossa siepataan ARP-viestejä käyttäjän ja tukiaseman väliltä (komento 8). [12]

sudo aireplay-ng -3 -b 00:02:CF:A1:A1:E2 mon0 (8)

Käyttäjän ja tukiaseman välinen verkkoliikenne määrittelee, kuinka kauan kyseisen hyökkäyksen käynnistämiseen menee. Yleensä hyökkäys käynnistyy varsin nopeasti, mutta voi kestää useampiakin minuutteja (kuva 11).

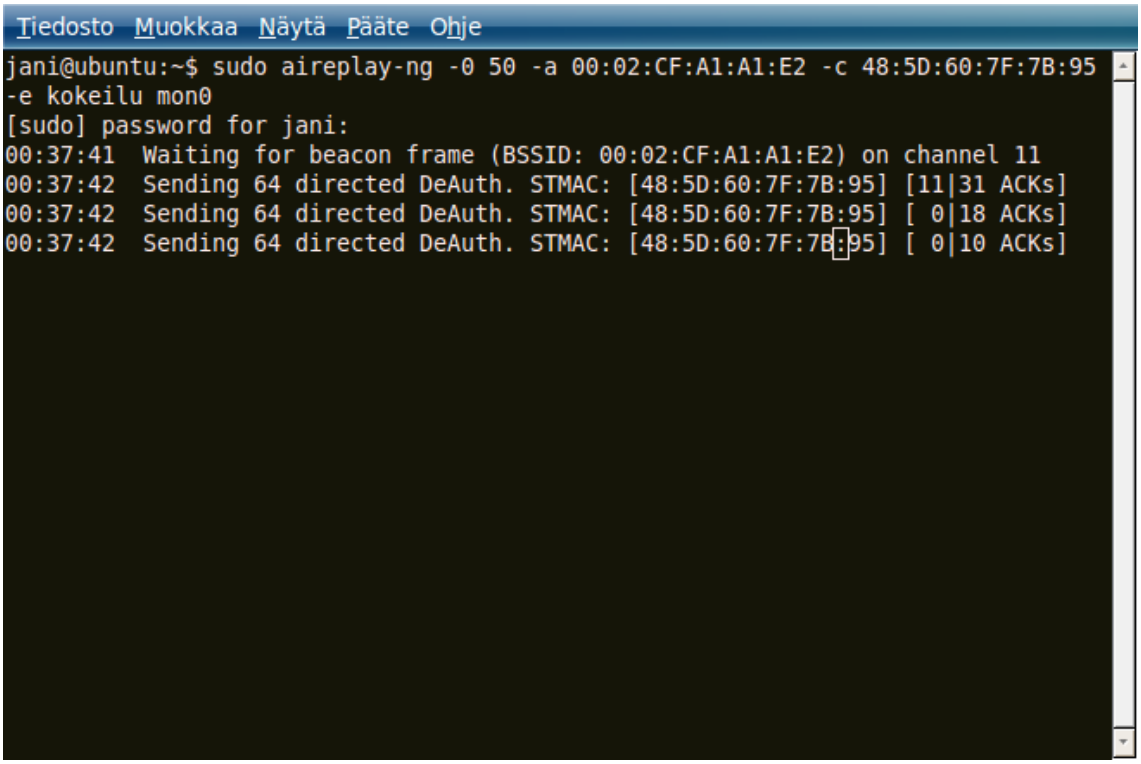


Kuva 11. ARP-replay hyökkäys käynnistetään tukiasemaa kohtaan.

Edellistä hyökkäystä voidaan nopeuttaa siten, että suoritetaan toisessa päätteessä vielä toinen hyökkäys nimeltä deautentikointihyökkäys (komento 9). Siinä ollaan tukiasemaan yhdistynyttä käyttäjää vastaan. [13]

sudo aireplay -0 50 -a 00:02:CF:A1:A1:E2 -c 48:5D:60:7F:7B:95 -e kokeilu mon0”. (9)

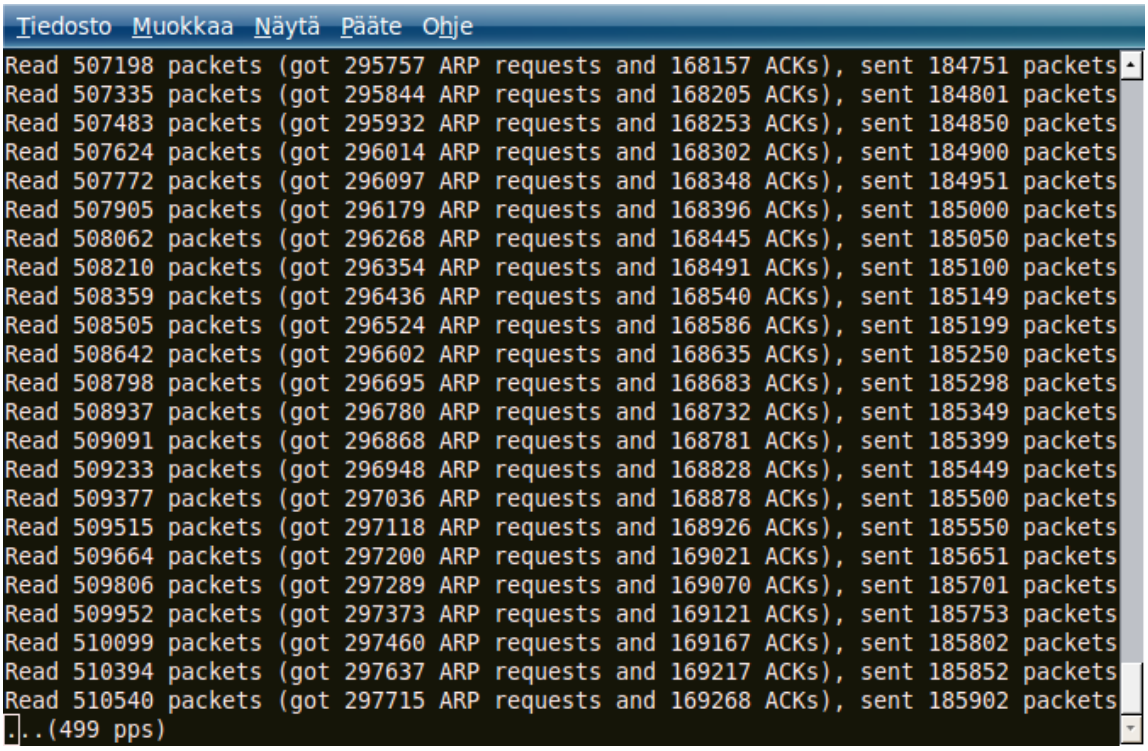
Tarkoituksena hyökkäyksessä on katkaista käyttäjän yhteys tukiasemaan hetkeksi, jonka jälkeen yhteys palaa takaisin käyttäjän ja tukiaseman välille (kuva 12).



Kuva 12. Aireplay-ng-ohjelma suorittaa deautentikointihyökkäystä käyttäjää vastaan.

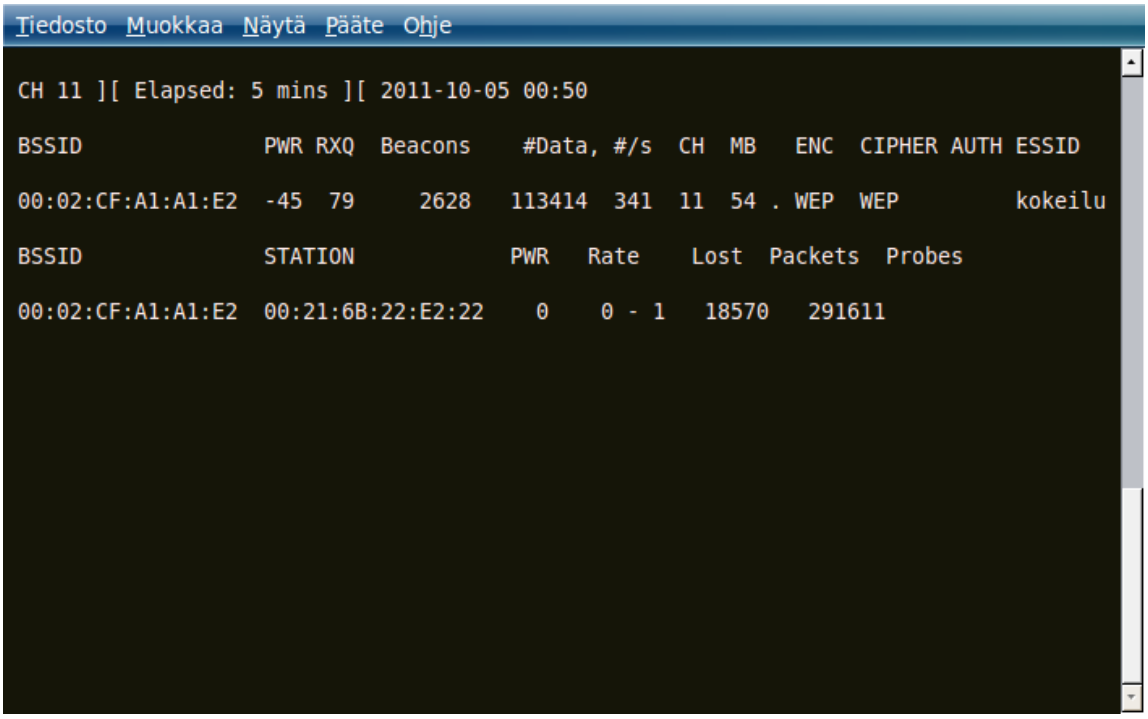
Ensimmäinen havainto tuli esille deautentikointihyökkäyksen aikana. Minikannettava, jossa on käyttöjärjestelmänä Windows XP, käyttäjän yhteys tukiasemaan katkaistiin hetkeksi, jonka jälkeen yhteys palasi. Toinen minikannettava, jossa on käyttöjärjestelmänä Windows 7, reagoi eri tavalla hyökkäykseen. Se sammutti WLAN-verkkokortin, jonka jälkeen se ei mennyt päälle kuin käynnistämällä järjestelmä uudelleen.

Hyökkäyksen jälkeen ARP-viestit saadaan siepattua, jolloin niitä voidaan alkaa lähettämään takaisin langattomaan verkkoon (kuva 13). Se aiheuttaa liikennettä langattomassa verkossa, jolloin siepattujen alustusvektori pakettien määrä kasvaa nopeammin.



Kuva 13. Langattomaan verkkoon lähetetään takaisin siepattuja ARP-viestejä.

Avataan vielä kolmas pääte, jossa nähdään airodump-ng-ohjelmalla, kuinka paljon alustusvektori pakettien määrä nousi. Huomataan, että alustusvektori pakettien määrä nousi 341 kappaletta sekunnissa (kuva 14).

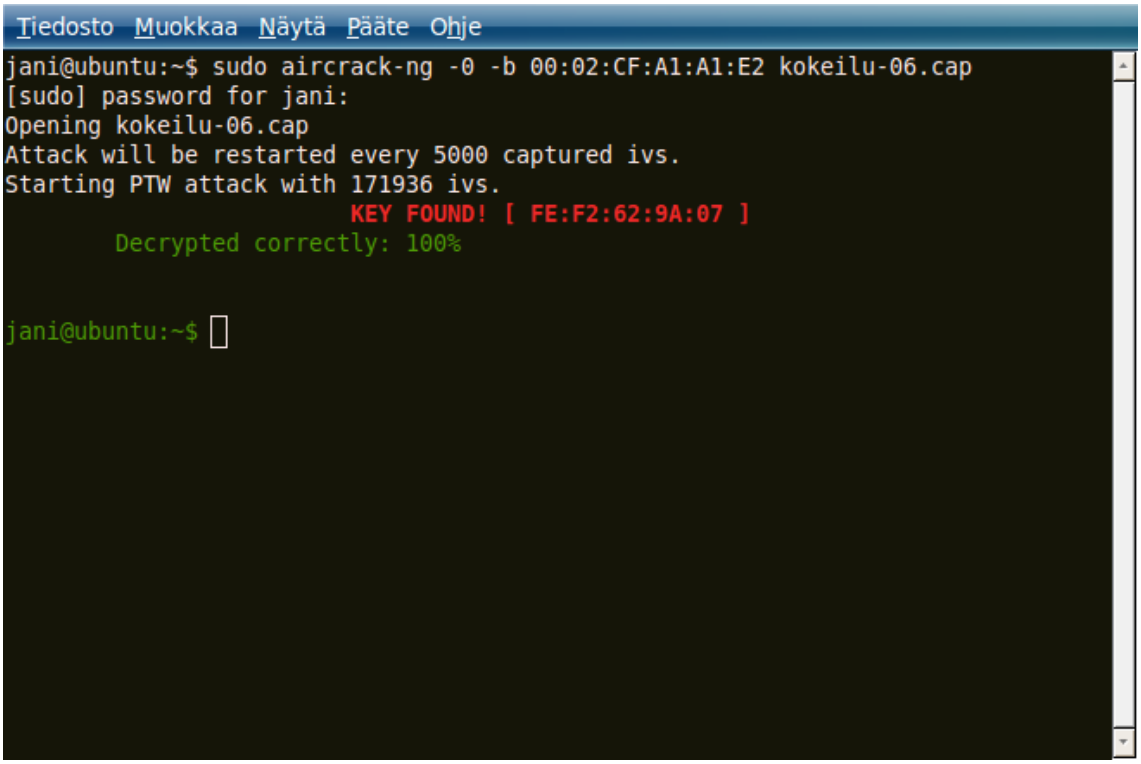


Kuva 14. Alustusvektori pakettien määrä kasvaa 341 pakettia sekunnissa.

Kun siepattujen alustusvektori pakettien määrä nousee, käynnistetään taustalle uudessa päätteessä aircrack-ng-ohjelma murtamaan WEP-salausavainta (komento 10). [14]

```
sudo aircrack-ng -0 -b 00:02:CF:A1:A1:E2 kokeilu-06.cap          (10)
```

Aircrack-ng-murtautumisohjelma aloittaa WEP-salausavaimen murtamisen cap-tiedostoon siepattujen alustusvektori pakettien avulla (kuva 15). Tämä onnistuu vain, jos alustusvektori paketteja on siepattu tarpeeksi. Jos paketteja ei ole tarpeeksi, siepattu ohjelma yrittää uudelleen, kun alustusvektori paketteja on siepattu 5000 kappaletta lisää cap-tiedostoon. Tämä toimenpide toistuu niin kauan, kunnes ohjelma on saanut murrettua WEP-salausavaimen. Tutkimus olosuhteissa WEP-salausavain murrettiin noin 4–6 minuutin sisällä pakettien sieppaamisesta alkaen.



Kuva 15. Aircrack-ng-ohjelma on purkanut salausavaimen.

Mahdollista on myös olla käyttämättä paketin lähettämistä, mutta silloin käyttäjän ja tukiaseman välinen datansiirtomäärä vaikuttaa alustusvektori pakettien sieppausnopeuteen. Jos dataa ei ole langattomassa verkossa tarpeeksi, alustusvektori pakettien sieppaus onnistuu vaikeammin. Sieppausnopeutta saadaan nostettua avaamalla esimerkiksi Internet-sivu, joka tuottaa datansiirtoa. Näin sieppausnopeus saadaan 100–300 paketin sekuntinopeuteen hetkellisesti. Tämä loppuu, kun Internet-sivun sisältö on saatu ladattua. Kun langattomassa verkossa on hidas liikenne, WEP-salausavaimen murtaminen voi kestää jopa 40 minuuttia.

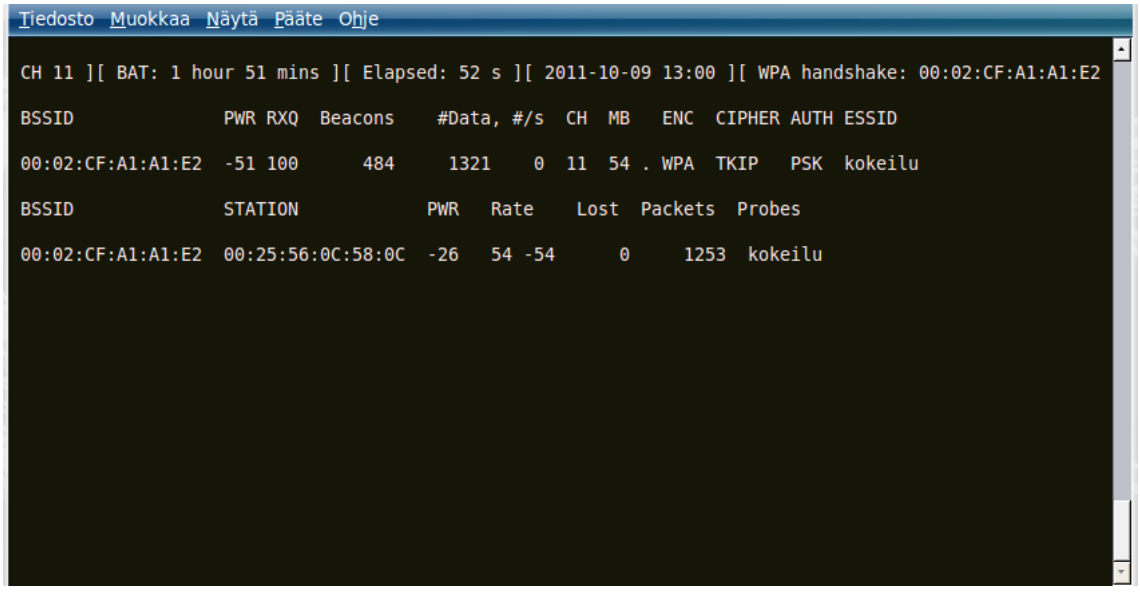
7.3 WPA- ja WPA2-salausavaimien purku

WPA- ja WPA2-salausprotokollan murtamiseen ei voi käyttää samoja keinoja kuin WEP-salausprotokollan murtamiseen. Salausavaimen voi murtaa, jos käyttäjä on yhdistynyt tukiasemaan ja salausavain on tarpeeksi yleinen. Yleinen salausavain voi löytyä esimerkiksi tavallisista arkiasioista, kuten käyttäjän nimestä.

Käyttäjä ja tukiasema tunnistavat toisensa niin sanotussa nelivaiheisessa kättelyssä. Sen avulla saadaan selville tukiasemaan yhdistyvän käyttäjän luotettavuus. Tähän käytetään airodump-ng-ohjelmaa, joka mahdollistaa tämän nelivaiheisen kättelytapahtuman sieppaamisen ja tallentamisen tiedostoon.

Kättelyn sieppaamiseksi käyttäjän pitää olla yhdistynyt tukiasemaan tai liittyä langattomaan lähiverkkoon, kun airodump-ng on käynnissä. Jos airodump-ng käynnistetään vasta, kun käyttäjä on yhdistynyt, pitää suorittaa käyttäjää vastaan deautentikointihyökkäys, jotta käyttäjän yhteys tukiasemaan katkaistaan ja yhdistyessä uudelleen saadaan siepattua kättelytapahtuma.

Tutkimuksissa tutkittiin WPA- ja WPA2-salausprotokollia, jotka käyttävät TKIP- ja AES-salauksia. Tämän aikana huomataan toinen havainto. Minikannettavalla, missä käyttöjärjestelmänä on Windows XP, käyttäjä yhdistyi tukiasemaan ja sitä vastaan saatiin molemmat nelivaiheiset kättelytapahtumat siepattua ja tallennettua (kuva 16). Minikannettavassa, jossa käyttöjärjestelmänä on Windows 7, käyttäjä yhdistyi tukiasemaan eikä sitä vastaan saatu kumpiakaan kättelytapahtumia siepattua.



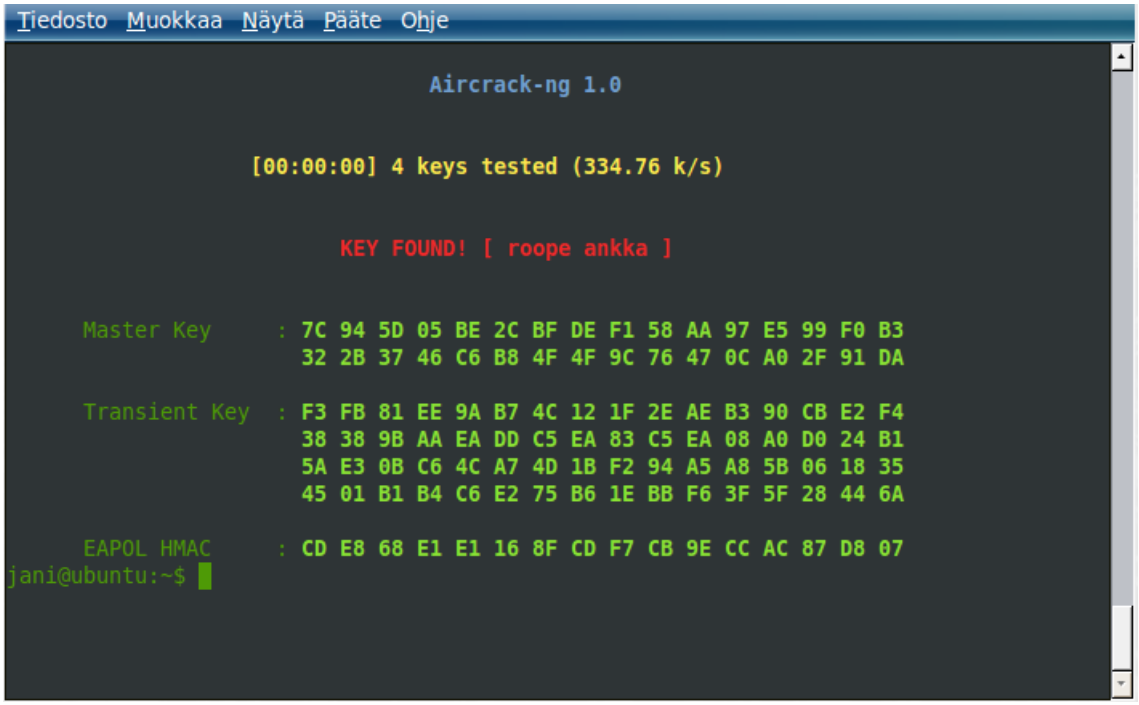
Kuva 16. Airodump-ng-ohjelma sieppaa WPA-kättelyn.

Siepattu kättely tallennetaan cap-tiedostoon, jota aircrack-ng-ohjelma käyttää salausavaimen murtamiseen. Käytettävä salausavain on tallennettu valmiiksi sanakirja

nimiseen tekstitiedostoon, jota aircrack-ng-ohjelma määritetään käyttämään (komento 11).

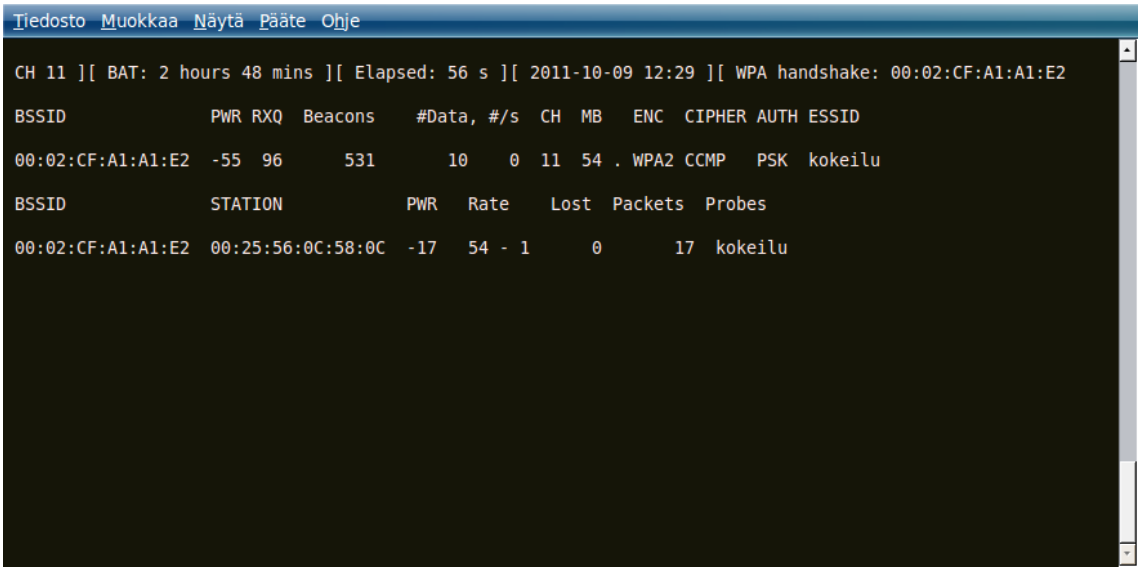
sudo aircrack-ng -0 -w sanakirja.txt -b 00:02:CF:A1:A1:E2 kokeilu-06.cap (11)

Aircrack-ng-ohjelma aloittaa salausavaimen murtamisen. Jos salausavain löytyy sanakirjatiedostosta, antaa se siitä ilmoituksen. Silloin aircrack-ng-ohjelma pysähtyy ja näyttää nopeuden, jolla sanoja käytiin läpi sanakirjalistasta (kuva 17).



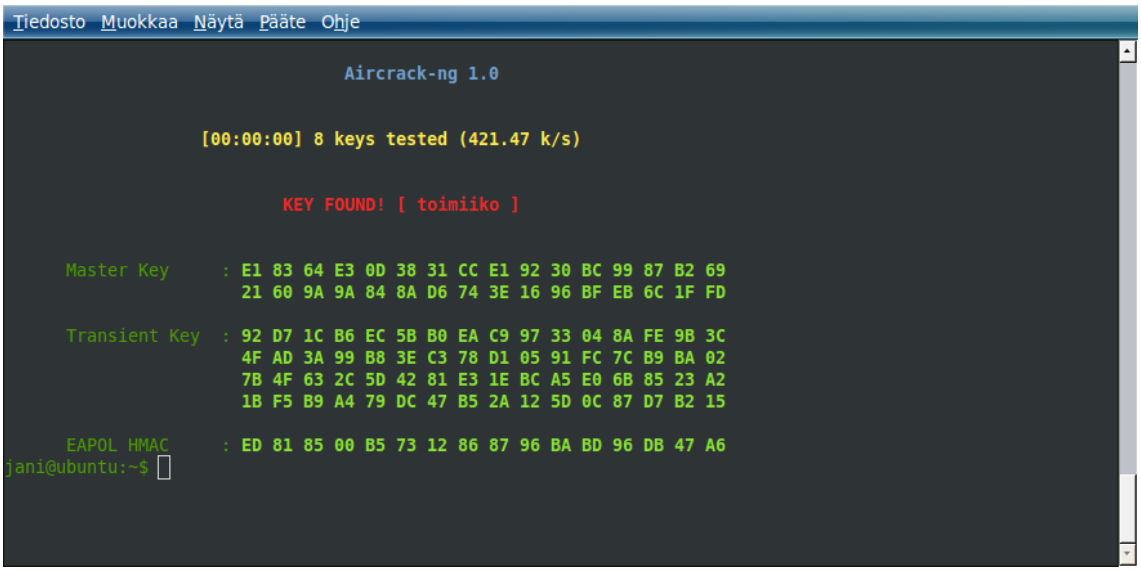
Kuva 17. Aircrack-ng-ohjelma on purkanut WPA-salausavaimen.

Seuraavaksi tehdään sama kuin WPA-salausprotokollassa eli siepataan nelivaiheinen kättely, kun käyttäjä yhdistyy tukiasemaan, mutta nyt WPA2-salausprotokollaa vastaan (kuva 18).



Kuva 18. Airodump-ng-ohjelma sieppaa WPA2-kättelyn.

Samaa sanakirjalistaa käytetään selvittääksemme WPA2-salausavaimen. Jos avain löytyy, ohjelma pysähtyy (kuva 19).



Kuva 19. Aircrack-ng-ohjelma on purkanut WPA2-salausavaimen.

Tutkimusten perusteella voidaan osoittaa, että WPA- ja WPA2-salausprotokollat ovat tarpeeksi turvallisia suojaustapoja. Salausavaimet eivät saa olla yleisiä ja helposti arvattavia, kuten esimerkiksi Walt Disney ja Volvo, jos haluaa suojata langattomia

verkkoja. Kyseisiä protokollia vastaan on olemassa hyökkäyksiä, mutta silti tarvitaan onnea, jotta salausavain löytyisi sanakirjalistoista.

Sanakirjahyökkäysmenetelmän käyttäminen on ajanhukkaa, kun muodostaa tarpeeksi vahvan salausavaimen, joka sisältää kirjaimia, numeroita, erikoismerkkejä ja on tarpeeksi pitkä, kuten esimerkiksi 3!9F4H^d57>#6£9ZöQ~’db*?+. Näissä tutkimusolosuhteissa sanakirjalistat olivat lyhyitä ja näin ollen salausavain tunnistetaan sanakirjalistasta. Näitä sanakirjalistoja on saatavissa Internetistä usean gigatavun kokoisina, joten niiden sisältämät sanamäärät ovat omaa luokkaansa.

8 JOHTOPÄÄTÖKSET

Työssä oli tarkoituksena tutkia, kuinka turvalliset salausprotokollat ovat. Keskityin ensisijaisesti WEP-salausprotokollan murtamiseen, mutta tutkin myös WPA- ja WPA2-salausprotokollia.

Tutkimusten aloittamisen kannalta tärkeää oli ohjelman valinta, jota käytettäisiin murtautumistutkimuksissa. Vaihtoehtoja oli useita eri ohjelmia Windowsin- ja Linuxin-käyttöympäristön puolelta. Päädyin aircrack-ng-murto-ohjelmaan ja Linuxin Ubuntuun, koska useat ohjelmat tukivat Linuxia kuin Windowsia. Ohjelmat, jotka tukivat Windows-ympäristöä, olivat rajoitettuja toiminnaltaan ja ominaisuuksiltaan tai niiden tuki oli lopetettu joitakin vuosia sitten. Omia haasteita toi aircrack-ng-ohjelmaan tutustuminen ja oppiminen.

WEP-salausprotokollan turvallisuudesta tutkimukset antoivat vahvan ja yksimielisen tuloksen, josta sai tehtyä vahvat johtopäätökset turvallisuuden kannalta. Puheet helposta murtamisesta ja heikkouksista pitivät paikkansa, koska salausavain oli hetkessä selvitetty tutkimuksessa olevalla tekniikalla ja saatavilla ohjelmistoilla.

WPA- ja WPA2-salausprotokollien murtamisessa tehtiin seuraavia havaintoja. Tämä niin kutsuttu nelivaiheinen kättely saatiin siepattua minikannettavalta, jossa käyttöjärjestelmä on Windows XP, kun taas Windows 7-käyttöjärjestelmällä varustettua minikannettavan kättelyä ei saatu kaapatuksi. Samoin deautentikointihyökkäys toimi Windows XP -minikannettavaan mutta Windows 7 sammutti verkkokortin. Näihin syynä on Windows 7:n paranneltu tietoturvallisuus.

Muuten voidaan olla samaa mieltä tutkijoiden kanssa, että WPA- ja WPA2-salausprotokollat ovat turvallisia salauskeinoja tietoliikenteen salaamiseen, kun käyttää vahvaa salausavainta. Vahvat langattoman verkon salausavaimet koostuvat pitkistä merkkijonoista, jotka sisältävät kirjaimia, numeroita ja erikoismerkkejä sekaisin. WPA2 käyttämää AES-salausta suositellaan käyttäjille.

Työtä voisi jatkaa lisäämällä RADIUS-pavelimen ja tutkia, tuoko se lisää turvallisuutta käytettäviin WEP-, WPA- ja WPA2-salausprotokolliin, jolloin käyttäjän todentaminen tapahtuukin palvelimelta.

LÄHTEET

[1] Thomas, Tom, Verkkojen tietoturva, Helsinki: Edita, 2004.

[2] Geier, Jim, Langattomat verkot, Helsinki: Edita, 2005.

[3] Broadband Wireless Exchange, 802.11g Wireless internet Access, 2001, viitattu 28.9.2011, http://www.bbwexchange.com/wireless_internet_access/802.11g_wireless_internet_access.asP .

[4] Puska, Matti, Langattomat lähiverkot, Jyväskylä: Talentum, 2005.

[5] Broadcom 802.11n: The Next-Generation Wireless LAN Technology, 2006, http://www.broadcom.com/collateral/wp/802_11n-WP100-R.pdf.

[6] Hakala, Mika; Vainio, Mika & Vuorinen, Olli, Tietoturvallisuuden käsikirja, Porvoo: WS Bookwell, 2006.

[7] Lewis, Wayne, LAN Switching and Wireless, The United States of America: Cisco Press, 2009.

[8] Mister_X, Airmon-ng, 2010, viitattu 7.10.2011, http://www.aircrack-ng.org/doku.php?id=airmon-ng/.

[9] Sleek, Aireplay-ng, 2010, viitattu 7.10.2011, http://www.aircrack-ng.org/doku.php?id=aireplay-ng/.

[10] Sleek, Airodump-ng, 2010, viitattu 7.10.2011, http://www.aircrack-ng.org/doku.php?id=airodump-ng/.

[11] Sleek, Fake authentication, 2010, viitattu 8.10.2011, http://aircrack-ng.org/doku.php?id=fake_authentication.

[12] Sleek, ARP Request Replay Attack, 2010, viitattu 8.10.2011, http://aircrack-ng.org/doku.php?id=arp-request_reinjection/.

[13] Sleek, Deauthentication, 2010, viitattu 8.10.2011, http://www.aircrack-ng.org/doku.php?id=deauthentication/.

[14] Mister_X, Aircrack-ng, 2011, viitattu 8.10.2011, http://aircrack-ng.org/doku.php?id=aircrack-ng/.